CLAIM LISTING

1. (Currently Amended) A method for securing software to reduce unauthorized use, the method comprising:

providing at least one authorized representative entity installed on or in a user device;

obtaining registration information corresponding to at least one user device;

generating an authentication code at least partially based on the registration information;

associating the authentication code with the software;

determining whether a current user device is authorized using the authorized representative entity installed on or in the user device at least partially based on the authentication code associated with the software and registration information associated with the current user device without requiring communication with a remote authorized representative entity; and

~~controlling access to~~ allowing the software to be launched and operable if the current user device is authorized.

2. (Original) The method of claim 1 wherein the software is self activating and self authenticating in conjunction with the authorized representative located on or in the user device.

3. (Original) The method of claim 1 wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book.

4. (Original) The method of claim 1 wherein the step of obtaining registration information is performed by the at least one authorized representative entity installed on or in the user device.

5. (Original) The method of claim 1 wherein the step of generating an authentication code is performed by the at least one authorized representative entity installed on or in the user device.

6. (Original) The method of claim 1 wherein the step of obtaining registration information is performed by a remotely located authorized representative entity.

7. (Original) The method of claim 1 wherein the step of generating an authentication code is performed by a remotely located authorized representative entity.

8. (Original) The method of claim 1 wherein the steps of obtaining, generating, associating, determining, and controlling are performed by a resident authorized representative entity installed on at least one user device.

9. (Original) The method of claim 8 wherein registration information associated with the current user device remains within a trusted network associated with the user device.

10. (Previously Presented) The method of claim 8 wherein registration information associated with the current user device is not communicated to any device other than the user device.

11. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed prior to transferring the software to the current user device.

12. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed concurrent with transferring the software to the current user device.

13. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed following transferring the software to the current user device.

14. (Original) The method of claim 11 wherein the steps of obtaining, generating, and associating are performed by a remote authorized representative entity.

15. (Original) The method of claim 1 wherein the authorized representative entity comprises a hardware device.

16. (Original) The method of claim 15 wherein the hardware device is a computer chip.

17. (Original) The method of claim 15 wherein the hardware device is integral with a CPU.

18. (Original) The method of claim 15 wherein the hardware device is a PC card.

19. (Original) The method of claim 15 wherein the hardware device is a microprocessor.

20. (Currently Amended) The method of claim 1 wherein the ~~steps~~step of ~~determining whether a current user device is authorized and controlling access to allowing~~ the software to be launched and operable ~~is~~are performed by the authorized representative entity installed on or in a user device.

21. (Original) The method of claim 1 wherein the authorized representative entity comprises software.

22. (Original) The method of claim 21 wherein the software is electronically distributed.

23. (Previously Presented) The method of claim 21 wherein the software is transferred to a user device directly from a local computer readable storage medium.

24. (Original) The method of claim 1 further comprising electronically distributing the software to a user.

25. (Original)The method of claim 1 wherein at least one authentication code is distributed with the software.

26. (Original) The method of claim 1 wherein the authentication code corresponds to a group of user devices.

27. (Original) The method of claim 26 wherein the authentication code corresponds to a manufacturer of a user device.

28. (Original) The method of claim 26 wherein the authentication code corresponds to a model of a user device.

29. (Original) The method of claim 1 wherein the authentication code corresponds to a unique user device.

30. (Canceled)

31. (Previously Presented) The method of claim 1 further comprising preventing transfer of at least a portion of the software to the current user device if the current user device is not authorized.

32. (Previously Presented) The method of claim 1 further comprising preventing the current user device from utilizing the software if the current user device is not authorized.

33. (Previously Presented) The method of claim 1 wherein the current user device comprises a secondary user device.

34. (Previously Presented) The method of claim 1 wherein the steps of obtaining, generating, and associating are at least partially performed by a primary user device and the steps of determining and controlling are performed by a secondary user device.

35. (Original) The method of claim 1 further comprising encrypting the authentication code.

36. (Original) The method of claim 1 further comprising encrypting the registration information.

37. (Previously Presented) The method of claim 1 further comprising associating an identifier with the software so that authentication is triggered only on user devices having a local and/or remote authorized representative entity, wherein user devices not recognizing the identifier are allowed unrestricted access to the software.

38. (Original) The method of claim 1 further comprising:
securing any means for generating the authentication code after generating the authentication code associated with the software.

39. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are at least partially performed by an authorized representative entity installed on or in a user device, the method further comprising:
modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software.

40. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are at least partially performed by a remote authorized representative prior to distribution of the software.

41. (Currently Amended) A method for securing software to reduce unauthorized use having an authorized representative entity installed on or in a user device, the method comprising:
determining whether the user device is authorized to access the software using the authorized representative entity installed on or in the user device; and
controlling access to the software based on whether the user device is determined to be authorized, wherein the authorized representative entity installed

on or in the user device controls access to the software without contacting a
remotely located authorized representative entity ~~if the user device is authorized~~.

42. (Previously Presented)The method of claim 41 wherein the software is self
authenticating in conjunction with the authorized representative located on or in the
user device.

43. (Original) The method of claim 41 further comprising:
determining whether the user device is authorized to access the software
using a remotely located authorized representative entity in combination with the
authorized representative entity installed on or in the user device.

44. (Original) The method of claim 41 wherein the authorized representative
entity comprises a computer chip.

45. (Original) The method of claim 41 wherein the authorized representative
entity is integral with the CPU.

46. (Original) The method of claim 41 wherein the authorized representative
entity comprises a PC card.

47. (Original) The method of claim 41 wherein the authorized representative
entity comprises program instructions executed by a microprocessor.

48. (Original) The method of claim 47 wherein the program instructions
comprise an operating system component.

49. (Original) The method of claim 47 wherein the program instructions
comprise an application program.

50. (Original) The method of claim 47 wherein the program instructions
comprise a driver for a secondary device.

51. (Original) The method of claim 41 wherein the step of determining whether
the user device is authorized comprises:

comparing registration information associated with the user device to registration information associated with the software.

52. (Original) The method of claim 51 wherein the registration information associated with the software is embedded within an authentication code.

53. (Original) The method of claim 51 wherein the registration information associated with the software is encrypted.

54. (Original) The method of claim 51 wherein the registration information includes hardware information.

55. (Original) The method of claim 54 wherein the registration information includes hardware information associated with a unique user device.

56. (Original) The method of claim 55 wherein the hardware information includes a serial number.

57. (Original) The method of claim 54 wherein the registration information includes hardware information associated with a group of user devices.

58. (Original) The method of claim 41 wherein the authorized representative entity is installed by a manufacturer of the user device.

59. (Previously Presented) The method of claim 41 wherein the authorized representative entity is installed from a local computer readable storage medium directly connected to the user device.

60. (Original) The method of claim 41 wherein the authorized representative entity is downloaded to the user device.

61. (Original) The method of claim 41 wherein the authorized representative entity is transferred to the user device from a network.

62. (Original) The method of claim 41 wherein the step of controlling access comprises preventing the software from being transferred to a second user device.

63. (Original) The method of claim 41 wherein the step of controlling access comprises preventing the software from being executed by the user device.

64. (Original) The method of claim 41 wherein the step of controlling access comprises providing limited access to the software.

65. (Original) The method of claim 41 wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book.

66. (Original) The method of claim 41 wherein the software comprises instructions for generating at least one authentication code at least partially based on registration information associated with the user device.

67. (Original) The method of claim 66 wherein the software comprises instructions for encrypting the authentication code.

68. (Currently Amended) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:
contacting a remote authorized representative entity only if the authorized representative entity installed on or in a user device is unable to determine whether the user device is authorized.

69. (Previously presented) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:
contacting a remote authorized representative only if the authorized representative entity installed on or in a user device determines that the user device is not authorized.

70. (Original) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:

obtaining registration information associated with the user device; and

comparing the registration information associated with the user device with registration information encoded in an authentication code associated with the software.

71. (Original) The method of claim 41 further comprising:

detecting an identifier associated with the software to trigger authentication functions performed by the authorized representative entity installed on or in the user device; and

performing the steps of determining whether the user device is authorized and controlling access to the software only if the identifier is detected.

72. (Original) The method of claim 41 further comprising:

automatically contacting a remote authorized representative based upon a triggering event to receive information.

73. (Original) The method of claim 72 wherein the information is selected from a group consisting of updates, upgrades, patches, marketing information, promotional information, quality assurance information, network monitoring and metering information, and error and usage information.

74. (Original) The method of claim 73 wherein the information updates the authorized representative entity installed on or in the user device.

75. (Original) The method of claim 73 wherein the information modifies the software.

76. (Original) The method of claim 72 wherein the triggering event is based on a user action.

77. (Currently Amended) The method of claim 72 wherein the automatic contact with the remote authorized representative is repeated.

78. (Currently Amended) A method for reducing unauthorized use of software, the method comprising:

associating at least one identifier with the software corresponding to a request for digital rights management;

distributing the software to a user;

detecting the at least one identifier using an authorized representative entity installed on or in a user device;

associating at least one authentication code with the software;

determining whether a user device is authorized to access the software; and

controlling access to the software based on whether the user device is authorized, wherein a local authorized representative entity installed on or in the user device allows an authorized user device or devices to access the software without requiring contact with a remote authorized representative entity.

79. (Original)The method of claim 78 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

80. (Original) The method of claim 78 further comprising encrypting the at least one authentication code.

81. (Original) The method of claim 78 further comprising:

obtaining registration information associated with at least one user device; and

generating the at least one authentication code at least partially based on the registration information.

82. (Previously Presented) The method of claim 81 further comprising encrypting the registration information.

83. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed before the step of distributing the software.

84. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and

associating the at least one authentication code are performed concurrent with the step of distributing the software.

85. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed subsequent to the step of distributing the software.

86. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed by an authorized representative entity installed on or in the user device.

87. (Original) The method of claim 81 wherein the step of generating the at least one authentication code is performed by an authorized representative entity installed on or in the user device, the method further comprising:
    securing the authentication code to resist user tampering.

88. (Original) The method of claim 87 wherein the step of securing comprises preventing the authorized representative entity installed on or in the user device from generating any more authentication codes for the software.

89. (Original) The method of claim 87 wherein the step of securing comprises encrypting the authentication code.

90. (Original) The method of claim 78 further comprising:
    determining whether an operational authorized representative entity is available locally;
    installing an authorized representative entity on or in the user device if an operational authorized representative entity is not available locally.

91. (Original) The method of claim 90 wherein the step of installing comprises transferring the authorized representative entity to the user device from a remote authorized representative entity.

92. (Previously Presented The method of claim 90 wherein the step of installing comprises transferring the authorized representative entity to the user device directly from a local computer readable storage medium.

93. (Original) The method of claim 90 wherein the software includes an authorized representative entity and wherein the step of installing comprises transferring the authorized representative entity to the user device from the software.

94. (Original) The method of claim 78 further comprising:
determining whether an operational authorized representative entity is installed on or in the user device; and
contacting a remote authorized representative entity if no operational authorized representative entity is installed on or in the user device.

95. (Original) The method of claim 94 wherein the remote authorized representative entity performs the steps of determining whether a user device is authorized and controlling access to the software.

96. (Original) The method of claim 78 further comprising:
obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed prior to the step of distributing the software to a user.

97. (Original) The method of claim 78 further comprising:
obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed concurrent with the step of distributing the software to a user.

98. (Original) The method of claim 78 further comprising:
obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed following the step of distributing the software to a user.

99. (Original) The method of claim 67 wherein the step of determining whether a user device is authorized is performed by a hardware device.

100. (Original) The method of claim 67 wherein the step of controlling access to the software comprises preventing the software from being transferred to the user device if the user device is not authorized.